Wireshark

- GUI (Graphical) – point and click

Display filters (after capture): Very detailed, like `http.request.method == "POST"`

Similarities

- Can **read/write .pcap** files.
- Can be used together: e.g., **capture with tcpdump** (lightweight) → **analyze later with Wireshark** (visual)
- Are **packet sniffers**, not IDS tools.

tcpdump

- CLI (command line interface) - type commands.

Capture filters (before capture): Simpler, like `port 80`